Joseph Silva Jr.

SNHU

CS 405: 8-2 Journal: Portfolio Reflection

12/15/2021

Adopting a security code standard, allows the project to be consistent when it comes to its development and its security features regardless of which individual from team is developing the section of code to push into the main branch of the project. With a strong and consistent security standard, a project will be protected from domestic and foreign threats to the system. The “Don’t leave security to the end” practice means do not put developing security measures at the end of the development of the project. Ignoring this practice can cause an issue with the project itself and/or the protection of the project due to unreliable code. Depending on the project and the safety set of code, the safety areas and the entire project might not be compatible with each other and thus might have to make a team start the project over in order to accommodate the security sections of code needed in the project.

While reviewing Confluence, I was able to see how threats are reviewed and evaluated. The threats are than placed into certain areas of threat levels. Being able to categorize the different types of threat levels, teams are able to manage their time in order to correct and develop defenses against these certain types of threats in order to protect the project against security threats, going over budget, and over time management.

In this new era, systems security features need to continue to evolve against the growing threat of attacks. The zero-trust policies have been implemented into a lot of government databases at least in my experience. Zero-trust policies are being implemented into systems and databases for civilian corporations and/or individual accounts to protect the funds and security of the data in these companies. These types of policies request triple A policies and encryptions to be accessed in order for even employees to view the data Overtime, these security policies have gone from a “fortress” to protect the company outside threats to a “labyrinth” design to protect the system by only allowing those with access keys to access the data.

A security policy needs to be able to adapt and update over time against the adapting and updating of attacks because a security system and an attacker both grow over time by their own successes and failures against each other. With the world data being more stored in the digital world, the increase and consistency of attacks will continue overtime and developers must also be able to adapt their products security features in order to combat the current attacks and the attacks of the future.

**CITATIONS:**

1. Bellairs, R. (n.d.). *What is secure coding?* Perforce Software. Retrieved December 4, 2021, from <https://www.perforce.com/blog/sca/what-secure-coding>.
2. Kueh, T(n.d). *Practical guide to zero-trust policy.* The Real Post. Retrieved December 15, 2021, from <https://threatpost.com/practical-guide-zero-trust-security/151912/>
3. Schiela, R. (n.d) *SEI CERT C++ Coding Standard*. Confluence . Retrieved December 15, 2021, fromhttps://wiki.sei.cmu.edu/confluence/pages/viewpage.action?pageId=88046682